Műszaki Tudományos Közlemények vol. 9. (2018) 211–214
https://doi.org/10.33894/mtk-2018.09.48
Hungarian: https://doi.org/10.33895/mtk-2018.09.48,
http://eda.eme.ro/handle/10598/30332

# VULNERABILITY ANALYSIS OF A SMART HEATING SYSTEM

Barnabás SÁNDOR

*Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Budapest, Hungary,*
*sandor.barnabas@gmail.com*

**Abstract**

The opportunities offered by the smart city and the smart home to create livelier cities and homes in cities of increasing populations. [1] Meanwhile, there may be more problems which the average user does not yet think about. Focusing on these issues will be of utmost importance for information security and IT security, as the development of technology may not be able to keep up with a society such technologies are used in. On a theoretical and practical level, I examine an intelligent heating system for IT vulnerability, as well as some cases of attacks against IoT in recent years.

**Keywords***: smart city, smart home, smart heating, vulnerability.*

## 1. Introduction

The most significant attack in the past few years on IoT devices was the Mirai botnet which occurred on 21 October 2016, and in which millions of devices, including infected IP cameras, routers, and DVRs attacked Dyn Inc.'s DNS services, causing its service to become unavailable. The biggest companies involved in the attack were Amazon, Netflix, Twitter, Spotify, Reddit, CNN, PayPal, Pinterest, Fox News, New York Times, the Guardian and Wall Street Journal publishers. [2][3]

Based on the analysis, approximately 1.2 million infected devices received an HTTP request generating 100 Gbps traffic to Dyn servers from nearly 164 countries, which also portrays the volume of the attack. [4]

## 2. Vulnerability examination

The purpose of this study is to investigate and exploit the Honeywell RFID100 Internet Infrastructure Gateway, the Honeywell Y87RF wireless thermostat system. In the course of the investigation, the following objectives were as follows:

– Exploring the Honeywell RFG100 Internet Gateway vulnerabilities;
– Possible damages to IT, business and personal;
– Formulation of protection proposals and solutions.

### 2.1. The operating principle of the system

The intelligent heating system provides convenience. The location is a holiday home in Lake Balaton, where there is no continuous human presence, such as at a time of a winter departure, when the heating is switched on and off remotely for the purpose of welcoming occasional guests.

For its operation, Honeywell's one-zone thermostat package, and smartphone (iOS or Android) or desktop computer is required, depending on Internet access and usage. The system can be controlled via the Internet, from anywhere in the World via a dial-up application or by logging in to a website. **Figure 1** shows the block diagram of the current operating system.

### 2.2. Description of the test

The primary purpose of the "gray box" vulnerability test was to capture, decode and manipulate incoming and outgoing network traffic by Honeywell RFG100 Internet Gateway. [6] Tools used:

– MikroTik RB951G-2HnD programmable router;
– MacBook Air 13 "Laptop (Model: A1466);
– Lenovo ThinkPad x201 laptop;
– WireShark - network packet analysis software;
– Nmap - network testing software;
– SSLsplit - SSL Certificate Counterfeit Script;
– ARPspoof - ARP attack script.

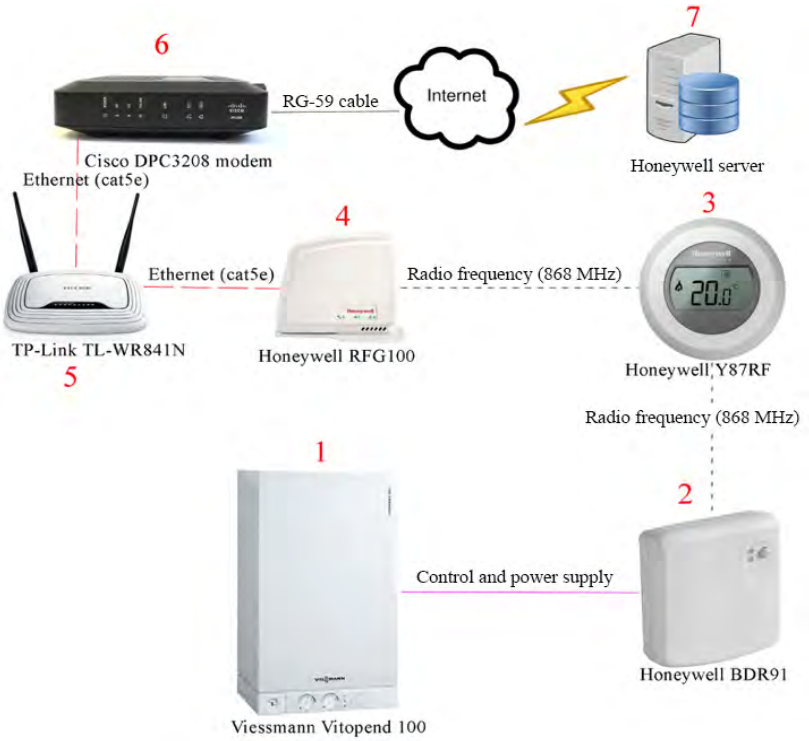


**Figure 1.** *Block and wiring diagram [5]*

### 2.3. Testing process

The TP-Link TL-WR841N router (**Figure 1.**) is replaced with a programmable MicroTik RB951G-2HnD router so that we can perform higher-level network management operations and then use the "Packet Sniffer" module to reflect the traffic of Honeywell Internet Gateway traffic and redirect Lenovo ThinkPad x201 for WireShark target software for monitoring purposes. By analyzing the MAC address of the Honeywell RFG100 Internet gateway, network traffic was targeted. When analysing network traffic, we obtained a more comprehensive picture of exactly which data packets are sent and received, and which servers are communicated with. **[7]**

The servers in **Table 1.** send and receive all the packets that are responsible for controlling the heating system. Since the gateway has no interface or access to the program code, we assume that it communicates with pre-programmed servers. Encrypted packets over port 443 in its internal ports (50103, 52575, 53200, 55615, 55879, 56475, 59134, 59878, 60410, 61038, 61667, 62575, 64029) open only when it is communicated.

**Table 1.** *Servers which the device communicates with*

| CNAME | IP |
|---|---|
| dns1.honeywell.com | 199.64.220.7 |
| dns1.honeywell.com | 199.61.24.26 |
| tccprod01.honeywell.com | 199.62.84.151 |
| tccprod01.honeywell.com | 199.62.84.152 |
| tccprod01.honeywell.com | 199.62.84.153 |

### 2.4. Software examination

During the software tests with Nmap, Zenmap and SSLsplit were investigated, which revealed that the basic TCP / UDP ports such as FTP (20, 21), SSH (22), TELNET (23), WEB (80, 8080) DNS (53) or 1 to 10000, are basically not open. During SSL certification, the device turned itself into standby mode and disconnected from the network. This suggests that these devices are equipped with HSTS protection. **[8]**

### 2.5. Physical examination

During the physical examination, the cover of the device was disassembled. The device is based on an SUI ML-2 94V-0 motherboard controlled by

a control chip Atmel AT91SAM9635-CU. The physical examination requires further future research.

## 3. Rules regarding the references

Damage can occur from an information security point of view (data theft); personal damage, property damage/crime or intent to defeat. The research highlights that if systems are not properly protected and configured, additional attacks may cause serious financial damage. Some examples of such incidents:

In the case of a drug store, a couple of tenths of a degree temperature difference may be significant in guaranteeing the quality of raw materials. For example, if a thermostatic system is attacked and elevated or the temperature is reduced, serious material damage to health can be caused.

In a similar type of attack - in case of a protected object - one can "force" a bodyguard to open the doors or windows of a room because the temperature has been changed to 30 degrees. So, you can get into the building through an open window.

The most serious cases include the malfunction of a baby monitor system, which suffered the best-known information security damages. In many cases, the attackers remotely accessed live view, so they could observe when no one was around. Thus, they could have kidnapped unprotected toddlers by night or day. **[9]**

There has also been an incident where a pacemaker has been attacked, and in such cases, the health status of the user can be directly affected. **[10]**

## 4. Prevention suggestions

The primary prevention step in each case is research, as it is a common problem that the average user is looking for the cheapest device. Before purchasing a device, one should look up the device type number or the posts and articles about it on the web as it may have known vulnerabilities. It is important to find out how long the manufacturer is undertaking software support for the device. If there has been no application/firmware update in years, one will not be prepared for it in the near future, which is also a security issue. Professionals are constantly investigating devices for vulnerabilities, so new ones appear almost daily. From this point on, an asset that has not been upgraded for up to a few months may pose a risk. Of course, there are zero-day vulnerabilities that have been present in the systems for years but have never been discovered. They pose a great risk in any case, as they possess a myriad of tools around the World.

## 5. Summary

In summary, it can be clearly stated that personal and property damage can be caused due to improperly secured and carelessly installed systems. In addition to the involvement of experts, it is important that users become trained in the safe use of the devices and their own safety awareness. It is not enough to install these tools; one has to learn how to use them and apply them into their life properly.

During the research, literary and online scientific and professional were used and processed in connection with vulnerabilities and their investigation. Various vulnerability testing tools and software have been used to meet the set goals.

During the investigation, it was found that the system was protected against particular attack modes. Basic network ports are only opened during communication and the SSL certificate is protected against forgery.

In the future we will carry out deeper research of hardware qualities and software, so the device will be examined at the control unit level, and in addition, we would also like to assess radio frequency communication.

### References

[1] MTA RKK NYUTI, IBM Magyarország Kft.: „Smart cities” tanulmány, 2011. május, ISBN 978-963-08-1739-4

[2] Thielman S., Johnston C.: *Major cyber-attack disrupts internet service across Europe and US.* The Guardian, 2016. www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service

[3] Mohit Kumar: *Mirai Botnet Itself is Flawed; Hacking Back IoTs Could Mitigate DDoS Attacks*. The Hacker News, 2016. www.thehackernews.com/2016/10/mirai-botnet-iot-malware.html

[4] Mohit Kumar: An Army of Million Hacked IoT Devices Almost Broke the Internet Today, The Hacker News, www.thehackernews.com/2016/10/iot-dyn-ddos-attack.html

[5] Self-made illustration

[6] IT Secure: *Sérülékenység vizsgálat (Etikus Hack)* www.itsecure.hu/etikus_hack

[7] Sándor B.: E*xamination of a man-in-the-middle attack in a wireless network* – Óbuda University BGK, thezis, 2017. ISBN 978-963-449-019-7

[8] Oriyano S. P.: *CEH v9 Study Guide*, John Wiley & Sons Inc., Indianapolis, 2016, 129-145, ISBN 978-1-119-25224-5
[9] Khyati Jain: *Caution! Hackers Can Easily Hijack Popular Baby Monitors to Watch Your Kids*, The Hacker News, 2015.09.03., www.thehackernews.com/2015/09/baby-monitor-hacking-tool.html
[10] Swati Khandelwal: *FDA Recalls Nearly Half a Million Pacemakers over Hacking Fears*. The Hacker News, 2017.08.31., www.thehackernews.com/2017/08/pacemakers-hacking.html